

**IN THE UNITED STATES DISTRICT COURT  
NORTHERN DISTRICT OF TEXAS**

JOHN DOE (a pseudonym) )  
On behalf of himself and all others similarly )  
situated )  
)  
)  
)  
Plaintiff, )  
)  
vs. )  
)  
)  
AVID LIFE MEDIA, INC. )  
a corporation, )  
)  
Defendant. )

**Case Number: 3:15-cv-2750**

**JURY TRIAL DEMANDED**

**CLASS ACTION COMPLAINT**

NOW COMES the Plaintiff John Doe (a pseudonym), on behalf of himself and all others similarly situated, and for his class action complaint states as follows:

**NATURE OF THE ACTION**

1. Plaintiff bring this class action as a result of a breach of the security system of Defendant AVID LIFE MEDIA INC. (“ALM” or “Defendant”) governing electronic transactions, resulting in compromised security of Plaintiff’s and Class Members’ personal financial and other information. Upon information and belief such personal information included, but was not limited to, the putative Class Members’ (hereafter “Class Members”) names, addresses, credit or debit card number, the card’s expiration date, and/or the card’s CVV (a three-digit security code), credit card transactions, users’ sexual preferences and fantasies, and email addresses (“Personal Information”).

2. On or about July 15 of this year, and at times prior, ALM’s databases were compromised, with the result that Personal Information of Plaintiff and Class Members’ Personal Information was used or is at risk of use in fraudulent transactions around the world,

as well as other invidious exposure. Upon information and belief, Defendant maintains or maintained information, including Personal Information, regarding nearly 37 million subscribers, and Defendant's security failures affected the credit and debit card of millions of customers, including Plaintiff and Class Members. One of the primary purposes of Defendants product and services was confidentiality and anonymity.

3. Upon information and belief, the security breach and theft of Personal Information was caused by Defendant's violations of its obligations to abide by the best practices and industry standards concerning the security of its payment processing systems and the computers associated therewith as set forth, for example, in Payment Card Industry Security Standards Council Data Security Standards ("PCI DSS") and the decisions of the Federal Trade Commission ("FTC") concerning protection of consumer financial information. Upon information and belief, hackers deliberately targeted Defendant's servers and collected names, usernames, passwords, email addresses, phone numbers, mailing addresses, and credit card numbers and expiration dates, credit card transactions, and other information. Upon information and belief, Defendant was also warned that the Personal Information would be released:

TIME'S UP!

Avid Life Media has failed to take down Ashley Madison and Established Men. We have explained the fraud, deceit, and stupidity of ALM and their members. Now everyone gets to see their data.

Find someone you know in here? Keep in mind the site is a scam with thousands of fake female profiles. See ashley madison fake profile lawsuit; 90-95% of actual users are male. Chances are your man signed up on the world's biggest affair site, but never had one. He just tried to. If that distinction matters.

Find yourself in here? It was ALM that failed you and lied to you. Prosecute them and claim damages. Then move on with your life. Learn your lesson and make amends. Embarrassing now, but you'll get over it.

Any data not signed with key 6E50 3F39 BA6A EAAD D81D ECFF 2437 3CD5 74AB AA38 is fake.

4. After learning of the security breach, Defendant failed to notify Plaintiff and the putative Classes in a timely manner and failed to take other reasonable steps to inform them of the nature and extent of the breach. As a result, Defendant prevented Plaintiff and the putative Class Members from protecting themselves from the breach and caused Plaintiff and Class Members to suffer financial loss and emotional distress.

5. On or about August 18 of this year, the Personal Information of Plaintiff and Class Members was actually released to the public and was put on several websites. On or about August 20 of this year, additional Personal Information of Plaintiff and Class Members was similarly released. Despite being told that it could prevent the release of Personal Information of Plaintiff and Class Members, Defendants allowed such Personal Information to be released to the public and did not notify Plaintiff and Class Members about the threat of the release of Personal Information or the actual release of Personal Information. Upon information and belief, in an internal company file called “Areas of concern – customer data.docx,” an unnamed employee at the company lists technical issues that could lead to a data breach occurring, as well the legal problems that may come with that. Under a section called “Data leak/thrift issues [sic],” the author lists customer data being exposed by phishing or SQL injection being a possible problem, when malicious requests are punched into an entry field, typically in order to dump the site database. Another employee worried about remote code execution—when an attacker can run code on a victims computer over the internet—and yet another employee pointed to employees being infected with malware, “allowing hackers access to our user data.”

6. Plaintiff, on behalf of himself and all others similarly situated, asserts the following claims: Violations of the Stored Communications Act (“SCA”), 18 U.S.C. § 2702; negligence; breach of implied contract; breach of contract, violations of the Texas Deceptive

Trade Practices-Consumer Protection Act (“DTPA”), under Section 17.45(4) of the Texas Business and Commerce Code and the substantially similar statutes of the other states in which Defendant conducts business, the Texas Identity Theft Enforcement Protection Act (TITEPA) because it is a “tie-in” statute as provided under Section 521.152 of the Texas Business and Commerce Code and the substantially similar statutes of the other states in which Defendant conducts business, and intentional infliction of emotional distress and the substantially similar statutes of the other states in which Defendant conducts business.

### **JURISDICTION AND VENUE**

7. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1331, which confers upon the Court original jurisdiction over all civil actions arising under the laws of the United States, and pursuant to 18 U.S.C. § 2707. This Court has supplemental jurisdiction over Plaintiff’s and Class Members’ state law claims under 28 U.S.C. § 1367.

8. In addition, this Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332(d)(2)(A) because this case is a class action where the aggregate claims of all Members of the putative Classes are in excess of \$5,000,000.00, exclusive of interest and costs, and many of the Members of the putative Classes are citizens of different states than Defendant. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332(d).

9. Venue is properly set in this District pursuant to 28 U.S.C. § 1391(b) since Defendant transacts business within this judicial district. Likewise, a substantial part of the events giving rise to the claim occurred within this judicial district.

### **PARTIES**

10. Plaintiff John Doe (a pseudonym) is an adult male domiciled in Austin, Texas and is a citizen of Texas. Plaintiff and Class members provided Personal Information to Defendant with a heightened expectation of privacy due to the nature of Defendant’s products

and services. Additionally, Class Members provided Personal Information to Defendant in order to effectuate a “paid-delete” of any of their personal information in Defendant’s possession, including Personal Information, as promised by Defendant. On information and belief Doe’s Personal Information was compromised as a result of Defendant’s security failures. As a result of such compromise, Doe suffered losses and damages in an amount yet to be completely determinable as such losses and damages are ongoing.

11. On information and belief Defendant is a corporation organized under Canadian law with its headquarters and principal place of business in Toronto, Canada.

### **FACTUAL BACKGROUND**

12. Plaintiff repeats, realleges, and incorporates paragraphs 1-11 in this Complaint as if fully set forth herein.

13. Defendant is a merchant that owns, operates, and controls social networking services, including a site on the Internet branded as “Ashley Madison”.

14. Upon information and belief, Defendant’s data breach has impacted millions of its customers nationwide within the United States.

15. Hackers accessed a database owned, operated, or controlled by ALM that processes, stores, or utilizes information regarding Personal Information, including ALM transactions, with account numbers, expiration dates, card holder names, credit card transactions, users’ sexual preferences and fantasies, email addresses, and/or other information, on information and belief. Hackers publicly exposed such personal information on both August

16. Class Members contacted Defendant to accept Defendant’s offer to “paid-delete” any personal information, including Personal Information, in Defendant’s possession; in other words, Defendant promised to delete such information for a fee (\$19, on information and belief).

17. Defendant broke such promise to the Class Members, who also sought a “paid-delete.”

18. Upon information and belief, the Defendant accepts customer payments for services through credit and debit cards issued by members of the payment card industry (“PCI”) such as Visa or MasterCard.

19. In 2006, the PCI members established a Security Standards Counsel (“PCI SSC”) as a forum to develop PCI Data Security Standards (“PCI DSS”) for increased security of payment processing systems.

20. The PCI DSS provides, “If you are a merchant that accepts payment cards, you are required to be compliant with the PCI Data Security Standard.” Defendant, of course, is a merchant that accepts payment cards.

21. The PCI DSS requires a merchant to:

a. **Assess**—identify cardholder data, take inventory of IT assets and business processes for payment card processing, and analyze them for vulnerabilities that could expose cardholder data.

b. **Remediate**—fix vulnerabilities and do not store cardholder data unless needed.

c. **Report**—compile and submit required remediation validation records (if applicable) and submit compliance reports to the acquiring bank and card brands with which a merchant does business.

22. Additionally, since 1995, the FTC has been studying the manner in which online entities collect and use personal information and safeguards to assure that online data collection practice is fair and provides adequate information privacy protection. The result of this study is the FTC Fair Information Practice Principles. The core principles are:

a. **Notice/Awareness**--Consumers should be given notice of an entity's information practices before any personal information is collected from them. This requires that companies explicitly notify of some or all of the following:

- Identification of the entity collecting the data;
- Identification of the uses to which the data will be put;
- Identification of any potential recipients of the data;
- The nature of the data collected and the means by which it is collected;
- Whether the provision of the requested data is voluntary or required; and
- The steps taken by the data collector to ensure the confidentiality, integrity and quality of the data.

b. **Choice/Consent**--Choice and consent in an online information-gathering sense means giving consumers options to control how their data is used with respect to secondary uses of information beyond the immediate needs of the information collector to complete the consumer's transaction.

c. **Access/Participation**--Access as defined in the Fair Information Practice Principles includes not only a consumer's ability to view the data collected, but also to verify and contest its accuracy. This access must be inexpensive and timely in order to be useful to the consumer.

d. **Integrity/Security**--Information collectors should ensure that the data they collect is accurate and secure. They should improve the integrity of data by cross-referencing it with only reputable databases and by providing access for the consumer to verify it. Information collectors should keep their data secure by protecting against both internal and external security threats. They should limit access within their company to

only necessary employees to protect against internal threats, and they should use encryption and other computer- based security systems to stop outside threats.

e. **Enforcement/Redress--**In order to ensure that companies follow the Fair Information Practice Principles, there must be enforcement measures. The FTC identifies three types of enforcement measures: self-regulation by the information collectors or an appointed regulatory body; private remedies that give civil causes of action for individuals whose information has been misused to sue violators; and government enforcement, which can include civil and criminal penalties levied by the government.

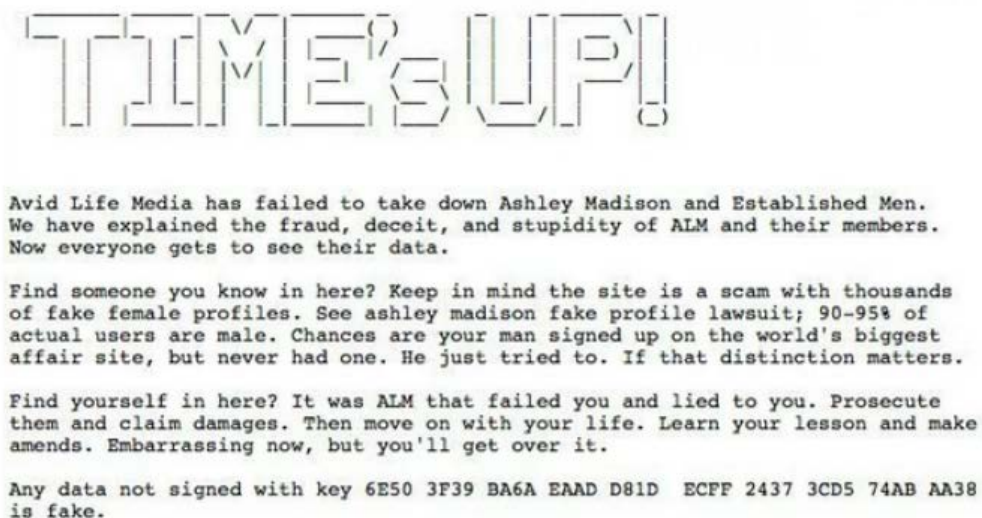
23. On information and belief, Defendant failed to adequately analyze its computer systems for vulnerabilities that could expose cardholder data. Defendant further failed to fix the vulnerabilities in its computer systems which allowed Plaintiff's and Class Members' Personal Information to become compromised.

24. Additionally, on information and belief, Defendant unlawfully collected consumer financial data for marketing purposes beyond the needs of specific transactions, in order to accrue financial benefit at the risk and likelihood of compromising consumers' Personal Information.

25. On or about July 15 of this year, and at times prior, ALM's databases were compromised, with the result that Personal Information of Plaintiff and Class Members' Personal Information was used or is at risk of use in fraudulent transactions around the world, as well as other invidious exposure. Upon information and belief, Defendant maintains or maintained information, including Personal Information, regarding nearly 37 million subscribers, and Defendant's security failures affected the credit and debit card of millions of customers, including Plaintiff and Class Members. One of the primary purposes of Defendants product and services was confidentiality and anonymity.



26. Upon information and belief, the security breach and theft of Personal Information was caused by Defendant's violations of its obligations to abide by the best practices and industry standards concerning the security of its payment processing systems and the computers associated therewith as set forth, for example, in Payment Card Industry Security Standards Council Data Security Standards ("PCI DSS") and the decisions of the Federal Trade Commission ("FTC") concerning protection of consumer financial information. Upon information and belief, hackers deliberately targeted Defendant's servers and collected names, usernames, passwords, email addresses, phone numbers, mailing addresses, and credit card numbers and expiration dates, credit card transactions, and other information. Upon information and belief, Defendant was also warned that the Personal Information would be released:



TIME'S UP!

Avid Life Media has failed to take down Ashley Madison and Established Men. We have explained the fraud, deceit, and stupidity of ALM and their members. Now everyone gets to see their data.

Find someone you know in here? Keep in mind the site is a scam with thousands of fake female profiles. See ashley madison fake profile lawsuit; 90-95% of actual users are male. Chances are your man signed up on the world's biggest affair site, but never had one. He just tried to. If that distinction matters.

Find yourself in here? It was ALM that failed you and lied to you. Prosecute them and claim damages. Then move on with your life. Learn your lesson and make amends. Embarrassing now, but you'll get over it.

Any data not signed with key 6E50 3F39 BA6A EAAD D81D ECFF 2437 3CD5 74AB AA38 is fake.

27. After learning of the security breach, Defendant failed to notify Plaintiff and the putative Classes in a timely manner and failed to take other reasonable steps to inform them of the nature and extent of the breach. As a result, Defendant prevented Plaintiff and the putative Class Members from protecting themselves from the breach and caused Plaintiff

and Class Members to suffer financial loss and emotional distress.

28. On or about August 18 of this year, the Personal Information of Plaintiff and Class Members was actually released to the public and was put on several websites. On or about August 20 of this year, additional Personal Information of Plaintiff and Class Members was similarly released. Despite being told that it could prevent the release of Personal Information of Plaintiff and Class Members, Defendants allowed such Personal Information to be released to the public and did not notify Plaintiff and Class Members about the threat of the release of Personal Information or the actual release of Personal Information. Upon information and belief, in an internal company file called “Areas of concern – customer data.docx,” an unnamed employee at the company lists technical issues that could lead to a data breach occurring, as well the legal problems that may come with that. Under a section called “Data leak/thrift issues [sic],” the author lists customer data being exposed by phishing or SQL injection being a possible problem, when malicious requests are punched into an entry field, typically in order to dump the site database. Another employee worried about remote code execution—when an attacker can run code on a victims computer over the internet—and yet another employee pointed to employees being infected with malware, “allowing hackers access to our user data.”

29. As a result, Defendant allowed Personal Information connected with millions of consumers’ credit cards and debit cards, including credit cards and debit cards of Plaintiff and Class Members and personal information related to the same, to become compromised for a period prior to July 15 of this year.

30. Additionally, Defendant was provided with Personal Information to in order to effectuate a “paid-delete” of any of their personal information in Defendant’s possession, including Personal Information, as promised by Defendant. In fact, the amount of Personal Information was increased because Defendant retained Personal Information related to the “paid-

delete” transaction itself. On information and belief Doe’s Personal Information was compromised as a result of Defendant’s security failures.

31. Plaintiff and Class Members are subject to continuing damage from having their Personal Information comprised as a result of Defendant’s inadequate systems and failures. Such damages include, among other things, the amount paid to Defendant to perform a “paid-delete” which Defendant did not perform or performed inadequately; out-of-pocket expenses incurred to mitigate the increased risk of identity theft and or fraud; credit, debit, and financial monitoring to prevent and/or mitigate theft, identity theft, and/or fraud incurred or likely to occur as a result of Defendant’s security failures; the value of their time and resources spent mitigating the identity theft and/or fraud; the cost of and time spent replacing credit cards and debit cards and reconfiguring automatic payment programs with other merchants related to the compromised cards; and irrecoverable financial losses due to unauthorized charges on the credit/debit cards of Defendant’s customers by identity thieves who wrongfully gained access to the Personal Information of Plaintiff and the Classes, the embarrassment of having Personal Information disclosed, the damage to marital relationships due to the breach, and the emotional distress of such breach. Plaintiff is in immediate danger of sustaining these direct injuries as the result of Defendants’ actions and inactions.

### **CLASS ACTION ALLEGATIONS**

32. Plaintiff repeats, realleges, and incorporates paragraphs 1-31 in this Complaint as if fully set forth herein.

33. Plaintiff brings this action on his own behalf and, pursuant to Rule 23 of the Federal Rules of Civil Procedure, on behalf of the following three (3) multi-state classes:

All persons in the United States who paid Defendant for “paid-delete” services which were improperly performed.

All persons in the United States whose Personal Information was subject to Defendant's security failures and who suffered damages and anticipate and/or are in immediate danger of suffering damages in the amount of fraudulent charges / unauthorized withdrawals made to their credit and/or debit cards or suffered damages and anticipate and/or are in immediate danger of suffering damages in the amount of overdraft charges made to their credit and/or debit cards.

All persons in the United States whose Personal Information was subject to Defendant's security failures and who have suffered or anticipate and/or are in immediate danger of suffering damages, loss, and/or expenses accruing due to Defendant's security failures.

Excluded from the Classes are Defendant and its affiliates, parents, subsidiaries, employees, officers, agents, and directors.

34. The Members of the Classes are so numerous that joinder of all Members is impracticable. On information and belief, millions of credit and/or debit cards may have been compromised, and the Members of the Classes are geographically dispersed. Disposition of the claims of the proposed Classes in a class action will provide substantial benefits to both the parties and the Court.

35. The rights of each member of the proposed Classes were violated in a similar fashion based upon Defendant's uniform wrongful actions and/or inaction.

36. The following questions of law and fact are common to each proposed Class Member and predominate over questions that may affect individual Class Members:

a. Whether Defendant failed to use reasonable care and commercially reasonable methods to secure and safeguard its customers' private financial and personal information;

b. Whether Defendant properly implemented its purported security measures to protect consumers' private financial and personal information from unauthorized

capture, dissemination and misuse;

c. Whether Defendant took reasonable measures to determine the extent of the security breach after it first learned of the same;

d. Whether Defendant's delay in informing consumers of the security breach was unreasonable;

e. Whether Defendant's method of informing consumers of the security breach and its description of the breach and potential exposure to damages as a result of the same was unreasonable;

f. Whether Defendant's conduct violated the Stored Communications Act, 18 U.S.C. § 2702;

g. Whether Defendant breached an implied contract with Class Members;

h. Whether Defendant's conduct violated the Texas Deceptive Trade Practices-Consumer Protection Act ("DTPA"), under Section 17.45(4) of the Texas Business and Commerce Code, and the substantively similar statutes of the other states where Defendant conducts business;

i. Whether Defendant's conduct violated the Texas Identity Theft Enforcement Protection Act (TITEPA) as a "tie-in" statute as provided under Section 521.152 of the Texas Business and Commerce Code and the substantially similar statutes of the other states in which Defendant conducts business;

j. Whether Defendant's intentionally inflicted emotional distress upon Plaintiff and Class Members, and the substantively similar statutes of the other states where Defendant conducts business; and

k. Whether Plaintiff and others Members of the Classes are entitled to compensation, monetary damages, equitable relief and injunctive relief, and, if so, the nature

and amount of such relief.

37. Plaintiff's claims are typical of the claim of absent Class Members. If brought individually, the claim of each Class Member would necessarily require proof of the same material and substantive facts, and seek the same remedies.

38. The Plaintiff is willing and prepared to serve the Court and the proposed Classes in a representative capacity. The Plaintiff will fairly and adequately protect the interest of the Classes and have no interests adverse to, or which directly and irrevocably conflicts with, the interests of other Members of the Classes. Further, Plaintiff has retained counsel experienced in prosecuting complex class action litigation.

39. Defendant has acted or refused to act on grounds generally applicable to the proposed Classes, thereby making appropriate equitable relief with respect to the Classes.

40. A class action is superior to other available methods for the fair and efficient adjudication of this controversy because individual claims by the Class Members are impractical, as the costs of prosecution may exceed what any Class Member has at stake.

41. Members of the Classes are readily ascertainable through Defendant's records of the transactions it undertook.

42. Prosecuting separate actions by individual Class Members would create a risk of inconsistent or varying adjudications that would establish incomparable standards of conduct for Defendant. Moreover, adjudications with respect to individual Class Members would, as a practical matter, be dispositive of the interests of other Class Members.

### **CAUSES OF ACTION**

#### **COUNT I – VIOLATION OF THE FEDERAL STORED COMMUNICATIONS ACT, 18 U.S.C. § 2702**

43. Plaintiff repeats, realleges, and incorporates paragraphs 1-42 in this Complaint

as if fully set forth herein.

44. The Stored Communications Act (“SCA”) contains provisions that provide consumers with redress if a company mishandles their electronically stored information. The SCA was designed, in relevant part, “to protect individuals’ privacy interests in personal and proprietary information.” S. Rep. No. 99-541, at 3 (1986), reprinted in 1986 U.S.C.C.A.N. 3555 at 3557.

45. Section 2702(a)(1) of the SCA provides that “a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service.” 18 U.S.C. § 2702(a)(1).

46. The SCA defines “electronic communication service” as “any service which provides to users thereof the ability to send or receive wire or electronic communications.” *Id.* at § 2510(15).

47. Through its payment processing equipment, Defendant provides an “electronic communication service to the public” within the meaning of the SCA because it provides consumers at large with credit and debit card payment processing capability that enables them to send or receive wire or electronic communications concerning their private financial information to transaction managers, card companies, or banks.

48. By failing to take commercially reasonable steps to safeguard sensitive private financial information, even after Defendant was aware that customers’ Personal Information had been compromised, Defendant has knowingly divulged customers’ private financial information that was communicated to financial institutions solely for customers’ payment verification purposes, while in electronic storage in Defendant’s payment system.

49. Section 2702(a)(2)(A) of the SCA provides that “a person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such service.” 18 U.S.C. § 2702(a)(2)(A).

50. The SCA defines “remote computing service” as “the provision to the public of computer storage or processing services by means of an electronic communication system.” 18 U.S.C. § 2711(2).

51. An “electronic communications systems” is defined by the SCA as “any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications.” 18 U.S.C. § 2510(4).

52. Defendant provides remote computing services to the public by virtue of its computer processing services for consumer credit and debit card payments, which are used by customers and carried out by means of an electronic communications system, namely the use of wire, electromagnetic, photooptical or photoelectric facilities for the transmission of wire or electronic communications received from, and on behalf of, the customer concerning customer private financial information.

53. By failing to take commercially reasonable steps to safeguard sensitive private financial information, Defendant has knowingly divulged customers’ private financial information that was carried and maintained on Defendant’s remote computing service solely for the customer’s payment verification purposes.

54. As a result of Defendant’s conduct described herein and its violations of



Section 2702(a)(1) and (2)(A), Plaintiff and putative Class Members have suffered injuries, including lost money and the costs associated with the need for vigilant credit monitoring to protect against additional identity theft. Plaintiff, on her own behalf and on behalf of the putative Classes, seek an order awarding themselves and the Classes the maximum statutory damages available under 18 U.S.C. § 2707 in addition to the cost for 3 years of credit monitoring services.

WHEREFORE Plaintiff and Class Members pray for Judgment in their favor and against Defendant on this Count I of their Complaint; for actual and compensatory damages; for punitive or exemplary damages; for punitive or exemplary damages; for punitive or exemplary damages; for injunctive relief; for costs, expenses and attorney fees as allowed by law; and for such other and further relief as this Court deems just and proper.

## **COUNT II – NEGLIGENCE**

55. Plaintiff repeats, realleges, and incorporates paragraphs 1-54 in this Complaint as if fully set forth herein.

56. Upon coming into possession of Plaintiff's and Class Members' Personal Information, i.e., private, non-public, sensitive financial information, Defendant had (and continues to have) a duty to exercise reasonable care in safeguarding and protecting the information from being compromised and/or stolen.

57. Defendant also had a duty to timely disclose to Plaintiff and Class Members that a breach of security had occurred and their Personal Information pertaining to their credit cards and/or debit cards had been compromised, or was reasonably believed to be compromised.

58. Defendant also had a duty to put into place internal policies and procedures designed to detect and prevent the theft or dissemination of Plaintiff's and

Class Members' Personal Information.

59. Defendant, by and through its above negligent acts and/or omissions, breached its duty to Plaintiff and Class Members by failing to exercise reasonable care in protecting and safeguarding their Personal Information which was in Defendant's possession, custody, and control.

60. Defendant, by and through its above negligent acts and or omissions, further breached its duty to Plaintiff and Class Members by failing to put into place internal policies and procedures designed to detect and prevent the unauthorized dissemination of Plaintiff and Class Members' Personal Information.

61. Defendant, by and through its above negligent acts and or omissions, breached its duty to timely disclose the fact that Plaintiff and Class Members' Personal Information had been or was reasonable believed to be have been compromised.

62. Defendant's negligent and wrongful breach of its duties owed to Plaintiff and Class Members, their Personal Information would not have been compromised.

63. Plaintiff's and Class Members' Personal Information was compromised and/or stolen as a direct and proximate result of Defendant's breach of its duties as set forth herein.

64. Plaintiff and Class Members have suffered actual damages including, but not limited to, having their personal information compromised, incurring time and expenses in cancelling their debit and/credit cards, activating new cards and re-establishing automatic payment authorizations from their new cards, and other economic and non-economic damages, including irrecoverable losses due to unauthorized charges on their credit/debit cards.

WHEREFORE Plaintiff and Class Members pray for Judgment in their favor and against Defendant on this Count II of their Complaint; for actual and compensatory damages;

for punitive or exemplary damages; for punitive or exemplary damages; for punitive or exemplary damages; for injunctive relief; for costs, expenses and attorney fees as allowed by law; and for such other and further relief as this Court deems just and proper.

### **COUNT III -- BREACH OF IMPLIED CONTRACT**

65. Plaintiff repeats, realleges, and incorporates paragraphs 1-64 in this Complaint as if fully set forth herein.

66. Plaintiff and Class Members were required to provide Defendant with their Personal Information in order to facilitate their credit card and/or debit card transactions.

67. Implicit in this requirement was a covenant requiring Defendant to take reasonable efforts to safeguard this information and promptly notify Plaintiff and Class Members in the event their information was compromised.

68. Similarly, it was implicit that Defendant would not disclose Plaintiff's and Class Members' Personal Information.

69. Notwithstanding its obligations, Defendant knowingly failed to safeguard and protect Plaintiff's and Class Members' Personal Information. To the contrary, Defendant allowed this information to be disseminated to unauthorized third parties.

70. Defendant's above wrongful actions and/or inaction breached its implied contracts with Plaintiff and Class Members, which in turn directly and/or proximately caused Plaintiff and Class Members to suffer substantial injuries.

WHEREFORE Plaintiff and Class Members pray for Judgment in their favor and against Defendant on this Count III of their Complaint; for actual and compensatory damages; for punitive or exemplary damages; for punitive or exemplary damages; for punitive or exemplary damages; for injunctive relief; for costs, expenses and attorney fees as allowed by law; and for such other and further relief as this Court deems just and proper.

**COUNT IV – VIOLATION OF TEXAS DECEPTIVE TRADE PRACTICES-  
CONSUMER PROTECTION ACT (“DTPA”), OF THE TEXAS BUSINESS AND  
COMMERCE CODE, AND SIMILAR STATUTES OF  
THE OTHER STATES WHERE DEFENDANT DOES BUSINESS**

71. Plaintiff repeats, realleges, and incorporates paragraphs 1-70 in this Complaint as if fully set forth herein.

72. Defendant violated the Texas Deceptive Trade Practices-Consumer Protection Act (“DTPA”), under Section 17.45(4) of the Texas Business and Commerce Code, and the substantially similar statutes of the other states in which it conducts business by failing to properly implement adequate, commercially reasonable security measures to protect customers’ private financial information, and by failing to immediately notify affected customers of the nature and extent of the security breach.

73. Defendant’s fraudulent and deceptive omissions and misrepresentations regarding the company’s security measures to protect customers’ private financial information and the extent of the breach of those security measures were intended to deceive and induce Plaintiff and the putative Class Members’ reliance on Defendant’s misrepresentations that their financial information was secure and protected when using debit and credit cards to shop at Defendant stores.

74. Defendant’s unlawful misrepresentations and omissions occurred in the course of conduct involving trade or commerce.

75. Defendant’s unlawful misrepresentations and omissions were material because Plaintiff and the other putative Class Members, if they had known the truth, would not have risked compromising their private financial information by using their debit or credit cards at Defendant stores. Plaintiff and the other putative Class Members would consider the omitted and misrepresented material facts important in making their purchasing

decisions.

76. Defendant's unlawful misrepresentations and omissions damaged Plaintiff and the other putative Class Members because Plaintiff and Class Members would not have chosen to expose their private financial information to a security breach and subsequent exploitation by the defrauders.

77. Plaintiff, therefore, prospectively asserts that by its above-described wrongful actions, inaction and/or omissions and the resulting data breach of Personal Information, Defendant knowingly and intentionally violated Section 17.50(a)(3) of the Texas Business and Commerce Code by engaging in the above-described unconscionable actions and/or unconscionable course of action; to wit, despite knowing of the security issues present in Defendants systems, failing to identify, implement, maintain and monitor the proper data security measures, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiff's and Class Members' Personal Information data which, as a direct and/or proximate result, was stolen and compromised in the Data Breach.

78. Defendant's above-described wrongful actions, inaction and/or omissions and the resulting Data Breach unfairly took advantage of the lack of knowledge, ability, and experience of Plaintiff and Class Members to a grossly unfair degree regarding Defendant's computer system and servers and Defendant's inability to safeguard and protect their Personal Information data; to wit, at the time Plaintiff and Class Members gave Defendants their Personal Information data in connection with purchasing of access and services, Plaintiff and Class Members did not know, and had no way of knowing, that Defendant was incapable of safeguarding and protecting their Personal Information data.

79. Concurrent with filing this Class Action Complaint, Plaintiff served a 60-day demand letter on Defendant under Section 17.505 of the Texas Business and Commerce Code.

Should this matter not be resolved to the satisfaction of Plaintiff, on behalf of himself and all Class Members, within the 60-day period, Plaintiff intends to amend this Class Action Complaint and formally assert this cause of action.

80. Plaintiff, individually and on behalf of the putative Classes, seek an order requiring Defendant to pay: monetary and punitive damages for the conduct described herein; three years of credit card fraud monitoring services for Plaintiff and Members of the putative Classes; and the reasonable attorney's fees and costs of suit of Plaintiff and Class Members; together with all such other and further relief as may be just.

WHEREFORE Plaintiff and Class Members pray for Judgment in their favor and against Defendant on this Count IV of their Complaint; for actual and compensatory damages; for punitive or exemplary damages; for punitive or exemplary damages; for punitive or exemplary damages; for injunctive relief; for costs, expenses and attorney fees as allowed by law; and for such other and further relief as this Court deems just and proper.

#### **COUNT V – BREACH OF CONTRACT**

81. Plaintiff repeats, realleges, and incorporates paragraphs 1-80 in this Complaint as if fully set forth herein.

82. Defendant promised the Class Members, for a fee of approximately \$19, to delete any of Plaintiff's/Class Member's personal information, including Personal Information, in Defendant's possession (the "paid-delete" service).

83. On information and belief, Defendant broke such promise, and did not delete some or all of Plaintiff's/Class Member's Personal Information in Defendant's possession, even after the payment of such fee.

84. Plaintiff have been damage thereby in the amount paid to the Defendant to perform a "paid-delete," and in the amount of other losses as previously stated.

WHEREFORE Plaintiff and Class Members pray for Judgment in their favor and against Defendant on this Count V of their Complaint; for actual and compensatory damages; for punitive or exemplary damages; for punitive or exemplary damages; for punitive or exemplary damages; for injunctive relief; for costs, expenses and attorney fees as allowed by law; and for such other and further relief as this Court deems just and proper.

**COUNT VI – INTENTIONAL INFLICTION OF EMOTIONAL DISTRESS**

85. Plaintiff repeats, realleges, and incorporates paragraphs 1-84 in this Complaint as if fully set forth herein.

86. Defendant acted intentionally or recklessly in failing to adequately secure Plaintiff and Class Members' Personal information despite knowing that there were security problems and failures and did nothing to remedy those problems and failures despite being aware of them. Moreover, despite being warned that Personal Information was compromised through a breach, Defendants intentionally or recklessly failed to mitigate such breach causing millions of users Personal Information to be released to the public. Such conduct was extreme and outrageous, especially in light of the confidential nature of the products and services that Defendant provides.

87. Defendant's actions caused Plaintiff and Class Members emotional distress directly related to their actions in the form of extreme and severe emotional distress over their marital relationship, societal status, reputation in the community, and other general distress resulting from Defendant's actions and inactions.

WHEREFORE Plaintiff and Class Members pray for Judgment in their favor and against Defendant on this Count VI of their Complaint; for actual and compensatory damages; for punitive or exemplary damages; for punitive or exemplary damages; for punitive or exemplary damages; for injunctive relief; for costs, expenses and attorney fees as allowed by law; and for such other and further relief as this Court deems just and proper.

**COUNT VII – TEXAS IDENTITY THEFT ENFORCEMENT PROTECTION ACT (TITEPA) AS A “TIE-IN” STATUTE AS PROVIDED UNDER SECTION 521.152 OF THE TEXAS BUSINESS AND COMMERCE CODE**

88. Plaintiff repeats, realleges, and incorporates paragraphs 1-87 in this Complaint as if fully set forth herein.

89. As plead in Count IV above, Plaintiff and Class Members are protected under the DTPA and Defendant is subject to the DTPA and subject to the provisions of the Texas Identity Theft Enforcement Protection Act (TITEPA) because it is a “tie-in” statute as provided under Section 521.152 of the Texas Business and Commerce Code.

90. Defendant stored Plaintiff’s and the Class’s Personal Information, including but not limited to sensitive personal information and personal identifying information such as their names, dates of birth, sometimes mother’s maiden names, account numbers, credit card numbers, physical conditions, and/or mental conditions, sexual preferences, sexual fantasies, physical addresses, and other information.

91. Plaintiff and the Class Members are “victims” under this act because their Personal Information is available on the internet and being perused by unauthorized individuals. Upon information and belief, Plaintiff and the Class Members’ information is also being used for profit and for blackmail purposes.

92. Defendant violated its duty to protect sensitive personal information by failing to implement and maintain reasonable procedures around the Personal Information, including taking protective actions when it knew the personal information was vulnerable, to protect the data from unlawful use.

93. Defendant also failed to destroy or arrange for the destruction of the personal information in a safe and secure manner in violation of this act. Further, Class Members who affirmatively paid Defendant to remove their personal data and received a guarantee that it was



removed were harmed. Defendant actually failed to safely and securely destroy that data and permitted it to be stolen by unauthorized users.

94. Defendant further violated this act by failing to notify Plaintiff and the Class immediately upon learning of the breach. Notice, if any, was given to Plaintiff and Class Members too late and not in accordance with this act.

95. As a natural and proximate cause of Defendant's violation of this act, Plaintiff and the Class Members were harmed and will continue to be harmed.

WHEREFORE Plaintiff and Class Members pray for Judgment in their favor and against Defendant on this Count VII of their Complaint; for actual and compensatory damages; for punitive or exemplary damages; for punitive or exemplary damages; for punitive or exemplary damages; for injunctive relief; for costs, expenses and attorney fees as allowed by law; and for such other and further relief as this Court deems just and proper.

#### **JURY TRIAL DEMAND**

Plaintiff and class members demand a jury trial as to all claims and issues triable of right by a jury.

#### **PRAYER FOR RELIEF**

WHEREFORE, Plaintiff and the Members of the proposed Classes pray that this Honorable Court do the following:

A. Certify the matter as a class action pursuant to the provisions of Rule 23 of the Federal Rules of Civil Procedure and order that notice be provided to all Class Members;

B. Designate Plaintiff as representative of the Classes and the undersigned counsel as Class Counsel;

C. Award Plaintiff and the Classes compensatory and punitive damages in an amount to be determined by the trier of fact;

- D. Award Plaintiff and the Classes statutory interest and penalties;
- E. Award Plaintiff and the Classes appropriate injunctive and/or declaratory relief;
- F. Award Plaintiff and the Classes their costs, prejudgment interest, and attorney fees; and
- G. Grant such other relief as is just and proper.

DATED: August 21, 2015.

/s/ James F. McDonough, III.

W. LEWIS GARRISON, JR.,  
*PHV forthcoming*  
lewis@hgdllawfirm.com  
TAYLOR C. BARTLETT,  
*PHV forthcoming*  
taylor@hgdllawfirm.com  
HENINGER GARRISON DAVIS, LLC  
2224 First Avenue North  
Birmingham, AL 35203  
Tel: 205-326-3336  
Fax: 205-326-3332

JAMES F. MCDONOUGH, III.  
*PHV forthcoming*  
jmcdonough@hgdllawfirm.com  
HENINGER GARRISON DAVIS, LLC  
3621 Vinings Slope, Suite 4320  
Atlanta, GA 30339  
Tel: 404-996-0869  
Fax: 205-326-3332

*Attorney for Named Plaintiff*

FERRER, POIROT & WANSBROUGH  
/s/ John T. Kirtley, III  
JOHN T. KIRTLEY, III  
Texas Bar no. 11534050  
2603 Oak Lawn Ave., Suite 300  
P. O. Box 199109  
Dallas, Texas 75219  
[jkirtley@lawyerworks.com](mailto:jkirtley@lawyerworks.com)  
(Asst. [molvera@lawyerworks.com](mailto:molvera@lawyerworks.com))  
(214) 521-4412 phone  
(214) 526-6026 facsimile  
*Attorney-In-Charge For Plaintiff*